HELSINGIN YLIOPISTO — HELSINGFORS UNIVERSITET — UNIVERSITY OF HELSINKI

Tiedekunta/Osasto — Fakultet/Sektion — Faculty	Laitos — Institution — Department
Matemaattis-luonnontieteellinen	Matematiikan ja tilastotieteen laitos

Tekijä — Författare — Author
Sampo Mustonen

Työn nimi — Arbetets titel — Title

Nullstellensatz

Oppiaine — Läroämne — Subject		
Matematiikka		
Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
Pro gradu -tutkielma	Toukokuu 2013	27 s.

Tiivistelmä — Referat — Abstract

Tässä työssä esitellään ja todistetaan nullstellensatz, eli Hilbertin nollajoukkolause. Todistuksessa oletetaan tunnetuksi kurssin 'Algebra I' asiat.

Nullstellensatz on algebran peruslauseen moniulotteinen yleistys. Se antaa Hilbertin vastaavuudeksi kutsutun bijektiivisen vastaavuuden varistojen ja radikaalien ideaalien välille. Monet algebrallisen geometrian keskeiset tulokset perustuvat nullstellensatziin.

Ennen nullstellensatzin todistamista, tässä työssä esitellään hieman ideaaleihin ja varistoihin liittyvää teoriaa. Lisäksi tässä työssä todistetaan Noetherin renkaisiin ja moduleihin liittyviä lauseita, joita tarvitaan nullstellensatzin todistamiseen. Lopussa todistetaan vielä nullstellensatzin seurauslauseita.

Avainsanat — Nyckelord — Keywords
Nullstellensatz, Hilbertin nollajoukkolause, algebrallinen geometria

Säilytyspaikka — Förvaringsställe — Where deposited
Kumpulan tiedekirjasto

Muita tietoja — Övriga uppgifter — Additional information

Nullstellensatz

Sampo Mustonen

Pro gradu -tutkielma
Matematiikan ja tilastotieteen laitos
Helsingin yliopisto

14. toukokuuta 2013

Sisältö

1 Johdanto

Nullstellensatz (lause 8.7), josta käytetään joskus myös nimeä Hilbertin nollajoukkolause, on algebran peruslauseen moniulotteinen yleistys. Algebran peruslauseen mukaan yhden muuttujan polynomi algebrallisesti suljetussa kunnassa määräytyy vakiokerrointa vaille nollakohdistaan kertaluvut huomioiden. Nullstellensatz taas sanoo, että polynomirenkaan radikaali ideaali määräytyy täysin nollajoukostaan. Nullstellensatz pätee missä tahansa algebrallisesti suljetussa kunnassa. Monet algebrallisen geometrian keskeiset tulokset perustuvat Nullstellensatziin. (Kahanpää, 2000)

2 Perusmääritelmiä

Tässä työssä oletetaan tunnetuksi kurssin Algebra I asiat. Nämä asiat löytyvät esimerkiksi kirjasta *Johdatus abstraktiin algebraan* (lähde 5).

Määritelmä 2.1 *Olkoon K kunta. Joukon $J \subset K[x_1, ..., x_n]$ varisto*

$$V(J) = \{x \in K^n \mid f(x) = 0 \ \forall f \in J\}.$$

Esimerkkejä algebrallisista varistoista löytyy luvusta 3.

Määritelmä 2.2 *Joukon $J \subset K^n$ ideaali*

$$I(J) = \{f \in K[x_1, ..., x_n] \mid f(x) = 0 \ \forall x \in J\}.$$

Joukon ideaali on aina ideaali.

Todistus: Aluksi todistetaan, että joukko $(I(J), +)$ on joukon $(K[x_1, ..., x_n], +)$ aliryhmä. Olkoon $g, h \in I(J)$. Nyt $g+h \in I(J)$, koska jos g ja h menevät nollaan joukossa J, niin niiden summa on myös nolla joukossa J. Käänteisalkiot kuuluvat joukkoon $I(J)$, koska polynomeilla $g, -g \in K[x_1, ..., x_n]$ on sama nollajoukko ($0 = -0$). Lisäksi neutraalialkio (0), kuuluu joukkoon $I(J)$, koska se on kaikkialla nolla. $(I(J), +)$ on siis joukon $(K[x_1, ..., x_n], +)$ aliryhmä.

Seuraavaksi todistetaan ideaalin toinen ehto: $\forall r \in K[x_1, ..., x_n], a \in I(J)$ pätee $ra \in I(J)$ ja $ar \in I(J)$. Tämä seuraa siitä, että ra (ja ar) menevät nollaan, kun toinen polynomeista menee nollaan ja tiedetään, että a menee nollaan joukossa J, koska se kuuluu joukkoon $I(J)$. □

Määritelmistä 2.1 ja 2.2 huomataan, että $J \subset I(V(J))$, koska joukko $V(J)$ on joukko, jossa kaikki joukon J polynomit saavat arvon nolla ja joukko $I(V(J))$ on joukko, johon kuuluvat kaikki polynomit, jotka saavat arvon nolla joukossa $V(J)$.

Määritelmä 2.3 *Renkaan R ideaali A on alkuideaali, jos $A \neq R$ ja kaikilla $x, y \in R$ pätee seuraava väite: jos $xy \in A$, niin $x \in A$ tai $y \in A$.*

Määritelmä 2.4 *Joukkojen $J_0, ..., J_n$ virittämä ideaali I on pienin sellainen ideaali, joka sisältää joukot $J_0, ..., J_n$. Joukkojen $J_0, ..., J_n$ virittämää ideaalia merkitään $\langle J_0, ..., J_n \rangle = I$. Vastaavalla tavalla määritellään myös muiden struktuurien ja alistruktuurien virittäminen.*

Määritelmä 2.5 *Olkoon K algebrallisesti suljettu kunta. Ideaalin $I \subset K[x_1, ..., x_n]$ radikaali*

$$r(I) = \{f \in K[x_1, ..., x_n] \mid f^n \in I \text{ jollain } n \in \mathbb{N}\}.$$

Jos $I = r(I)$, niin sanotaan, että ideaali on radikaali. Radikaalit ovat aina myös ideaaleja. Tämä seuraa suoraan nullstellensatzista (lause 8.7) ja määritelmän 2.2 todistuksesta.

Määritelmä 2.6 *Olkoon G ryhmä ja X joukko. Merkitään symbolilla X^X kaikkien kuvausten $X \to X$ joukkoa. Kuvausta $\varphi : G \to X^X$, missä $g \mapsto f_g$, kutsutaan ryhmän G vasemmanpuoleiseksi toiminnaksi joukossa X, jos se toteuttaa seuraavat ehdot:*

(T1): $f_e = id_X$, missä e on ryhmän G neutraalialkio.
(T2): $f_{gh} = f_g \circ f_h$, kaikilla $g, h \in G$.

Vastaavasti saadaan oikeanpuoleinen toiminta korvaamalla ehto (T2) ehdolla:

(T2'): $f_{gh} = f_h \circ f_g$, kaikilla $g, h \in G$.

Ryhmän toiminnasta käytetään merkintää $f_g(x) = g.x$. Tämä määritelmä soveltuu sellaisenaan myös monoidin toiminnan määrittelemiseen.

Määritelmä 2.7 *Renkaan $R \subset K[x_1, ..., x_n]$ ideaali $I \neq R$ on maksimaalinen, jos ei ole olemassa sellaista ideaalia X, jolle pätee $I \subsetneq X \subsetneq R$. Maksimaalinen moduli määritellään vastaavalla tavalla ja järjestysrelaatiolla varustetun joukon maksimaalinen alkio siten, että alkio a on maksimaalinen, jos ei ole olemassa alkiota b, jolle pätee $a < b$.*

Määritelmä 2.8 *Olkoon K kunta ja L kunnan K alikunta. Olkoon $x_1, ..., x_n \in K$. Alkiot $x_1, ..., x_n$ ovat algebrallisesti riippumattomia kunnan L suhteen, jos kaikilla $f \in L[X_1, ..., X_n]$ pätee, että $f(x_1, ..., x_n) = 0$ vain, jos $f = 0$.*

3 Affiinit algebralliset varistot

Algebrallinen geometria tutkii algebrallisia varistoja. Affiinilla algebrallisella varistolla tarkoitetaan polynomijoukon yhteisten nollakohtien joukkoa (määritelmä 2.1). Esimerkiksi koko avaruus K^n, tyhjä joukko ja yksiöt ovat Affiineja algebrallisia varistoja:

$$\varnothing = V(1)$$

$$K^n = V(0)$$

$$\{a\} = V(x_1 - a_1, ..., x_n - a_n),$$

missä $a = (a_1, ..., a_n) \in K^n$. Myös kahden (tai äärellisen monen) algebrallisen variston leikkaus ja yhdiste ovat myös algebrallisia varistoja:

$$V(X) \cap V(Y) = V(X \cup Y)$$

ja

$$V(X) \cup V(Y) = V(XY)$$

missä $X, Y \subset K[x_1, ..., x_n]$. (Kahanpää, 2000) Kertolaskulla XY tarkoitetaan tässä kertolaskua, jossa joukkojen X ja Y alkiot kerrotaan keskenään. Esimerkiksi $\{a, b\}\{c, d\} = \{ac, ad, bc, bd\}$.

Todistus (Leikkaus): Määritelmän 2.1 mukaan

$$V(X) \cap V(Y) = \{x \in K^n | f(x) = 0 \ \forall f \in X\} \cap \{x \in K^n | f(x) = 0 \ \forall f \in Y\}.$$

Joukkojen leikkauksessa alkion x tulee täyttää molempien joukkojen ehdot. Nyt saamme joukon muotoon:

$$\{x \in K^n | f(x) = 0 \ \forall f \in X \ ja \ f(x) = 0 \ \forall f \in Y\}.$$

Tämä taas saadaan muotoon:

$$\{x \in K^n | f(x) = 0 \ \forall f \in X \cup Y\} = V(X \cup Y). \ \square$$

Todistus (Yhdiste): Kuten edellisessä, yhdiste voidaan kirjoittaa muotoon:

$$\{x \in K^n | f(x) = 0 \ \forall f \in X\} \cup \{x \in K^n | f(x) = 0 \ \forall f \in Y\}.$$

Yhdisteessä alkion x täytyy täyttää vain toisen variston ehto:

$$\{x \in K^n | f(x) = 0 \ \forall f \in X \ tai \ f(x) = 0 \ \forall f \in Y\}.$$

Alkioiden tulo on nolla, kun toinen alkioista on nolla. Tämän seurauksena joukko voidaan kirjoittaa muotoon:

$$\{x \in K^n | f(x) = 0 \ \forall f \in XY\} = V(XY),$$

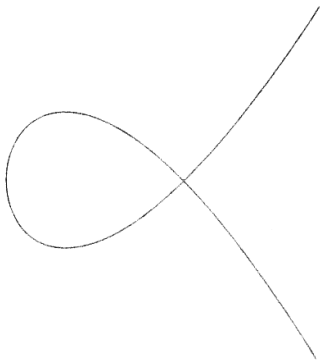
koska joukon XY alkiot ovat joukkojen X ja Y alkioiden tuloja, joten polynomi f saa arvon nolla, jos se saa arvon nolla toisessa tulon tekijöistä.

Lisäksi tulo on nolla vain, jos se saa arvon nolla toisessa tulon tekijöistä. Nyt on olemassa kaksi erilaista tapausta:

(1) $f(x) = 0$ kaikilla $f \in X$. Tällöin toinen tulontekijöistä on nolla.

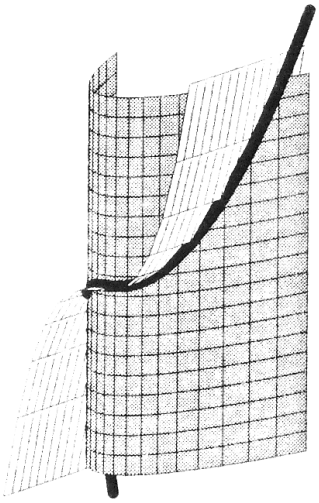
(2) $f(x) \neq 0$ jollain $f \in X$. Tulojoukossa XY tätä alkiota vastaavien tulojen $f(x)g(x)$ täytyy olla nolla kaikilla $g \in Y$. Tästä seuraa, että kaikilla $g \in Y$ $g(x) = 0$. □

Esimerkki 3.1 *Polynomin $y^2 - x^2 - x^3$ varisto, $V(y^2 - x^2 - x^3)$:*



Kuva 1: $V(y^2 - x^2 - x^3)$ (Kahanpää, 2000)

Esimerkki 3.2 *Polynomijoukon* $\{x^2 - y, x^3 - z\}$ *varisto on kierevä kuutioparabeli:*



Kuva 2: Kierevä kuutioparabeli (Kahanpää, 2000)

3.1 Zariskin topologia

Olkoon Z Affiinien algebrallisten varistojen komplementtien joukko. Nyt huomataan, että tyhjä joukko ja koko avaruus K^n kuuluvat joukkoon Z. Äärellisen monen joukon Z osajoukon leikkaukset kuuluvat myös joukkoon Z. Lisäksi voidaan todistaa, että mielivaltaiset joukon Z osajoukkojen yhdisteet kuuluvat joukkoon Z. Joukko Z toteuttaa siis joukon K^n topologian määritelmän. Tätä topologiaa kutsutaan joukon K^n Zariskin topologiaksi. Zariskin topologialla varustettua avaruutta K^n sanotaan affiiniksi avaruudeksi ($\mathbb{A}^n$). (Kahanpää, 2000)

Avaruuden $\mathbb{A}^n$ Zariskin topologian affiiniin algebralliseen varistoon $V \subset \mathbb{A}^n$ indusoimaa topologiaa sanotaan variston V Zariskin topologiaksi. Tässä topologiassa suljettuja joukkoja ovat variston V ja avaruuden $\mathbb{A}^n$ affiinien algebrallisten varistojen $W \subset \mathbb{A}^n$ leikkaukset $V \cap W$. Näitä leikkauksia sanotaan variston V affiineiksi alivaristoiksi. (Kahanpää, 2000)

Zariskin topologia on paljon karkeampi kuin euklidinen topologia, jokainen

Zariskin topologiassa suljettu joukko on suljettu myös euklidisessa topologiassa. Toisaalta Zariskin topologiassa avoimet joukot ovat tyhjää joukkoa lukuun ottamatta hyvin suuria, kuten käyrän tai pinnan komplementteja. Zariskin topologiassa kaikki avoimet joukot ovat tiheitä ja, tyhjää joukkoa lukuun ottamatta, rajoittamattomia. Kahden epätyhjän Zariskin topologiassa avoimen joukon leikkaus on aina epätyhjä, joten Zariskin topologia ei ole Hausdorff-topologia. (Kahanpää, 2000)

4 Modulit

Määritelmä 4.1 *Olkoon R ykkösellinen rengas. Vaihdannaista ryhmää $(M, +)$, jossa on määritelty renkaan R lineaarinen toiminta, kutsutaan R-moduliksi. Renkaan lineaarinen toiminta on renkaan kertolaskumonoidin $(R, \cdot)$ toiminta, joka toteuttaa seuraavat ehdot kaikilla $a, b \in R$ ja $x, y \in M$:*

(M1): $1.x = x$
(M2): $(ab).x = a.(b.x)$
(M3): $(a + b).x = a.x + b.x$
(M4): $a.(x + y) = a.x + a.y$

Rengasta R kutsutaan modulin kerroinrenkaaksi ja sen toimintaa skalaarikertolaskuksi. Modulia, jonka kerroinrengas on R, kutsutaan R-moduliksi.

Määritelmä 4.2 *Modulin M aliryhmä N on modulin M alimoduli, jos kaikilla $x, y \in N$ ja $a \in R$ pätee seuraavat ehdot:*

(AM1): $N \neq \emptyset$.
(AM2): $x - y \in N$.
(AM3): $a.x \in N$.

Määritelmä 4.3 *Vaihdannaisen renkaan R R-modulia A sanotaan R-algebraksi, jos siellä on määritelty R-bilineaarinen kertolasku $(x, y) \to x \cdot y$ kaikilla $x, y \in A$.*

Määritelmä 4.4 *Olkoon modulit M ja N saman modulin alimoduleita. Modulien M ja N summa $M + N = \{m + n \mid m \in M, n \in N\}$.*

Määritelmä 4.5 *Olkoon M ja N R-moduleita. Kuvaus $f : M \to N$ on homomorfismi, jos se toteuttaa seuraavat ehdot:*

(H1): $f(x + y) = f(x) + f(y)\ \forall x, y \in M$
(H2): $f(ax) = af(x)\ \forall x \in M,\ \forall a \in R$

Lause 4.6 *Homomorfismissa f alimodulin M alkukuva $f^{-1}(M)$ on alimoduli.*

Todistus: Olkoon $f : N \to M'$ homomorfismi, nissä N ja M' ovat R-moduleita. Olkoon M R-modulin M' alimoduli. Todistataan, että määritelmän 4.2 ehdot pätevät alkukuvassa $f^{-1}M$.

(AM1): Epätyhjän joukon alkukuva homomorfismissa on epätyhjä.
(AM2): Olkoon $a, b \in f^{-1}M$. Osoitetaan, että $a - b \in f^{-1}M$. Nyt $f(a - b) = f(a) - f(b) \in M$. Tästä seuraa, että $a - b \in f^{-1}M$.
(AM3): Olkoon $x \in R$ ja $a \in f^{-1}M$. Osoitetaan, että $x.a \in f^{-1}M$. Nyt tiedetään, että$f(x.a) = x.f(a) \in M$. Tästä seuraa, että $x.a \in f^{-1}M$.

Koska kaikki alimodulin ehdot pätevät alkukuvassa $f^{-1}M$, on alimodulin M alkukuva modulin N alimoduli. $\square$

5 Noetherin renkaat ja modulit

Määritelmä 5.1 *Noetherin rengas on rengas, jossa jokainen kasvava jono ideaaleja*

$$I_1 \subset I_2 \subset I_3 \subset \cdots ,$$

missä $I_i \neq I_{i+1}$, on äärellinen.

Määritelmä 5.2 *Olkoon A rengas ja M A-moduli. M on Noetherin moduli, jos se täyttää yhden seuraavista yhtäpitävistä ehdoista:*

(N1) Jokainen modulin M alimoduli on äärellisesti viritetty.
(N2) Jokainen kasvava jono modulin M alimoduleita,

$$M_1 \subset M_2 \subset M_3 \subset \cdots ,$$

missä $M_i \neq M_{i+1}$, on äärellinen.
(N3) Jokainen epätyhjä joukko S modulin M alimoduleita sisältää maksimaalisen alkion.

Todistus: Todistetaan määritelmän ehdot yhtäpitäviksi.

(N1) $\Rightarrow$ (N2): Olkoon $M_1 \subset M_2 \subset \cdots$ kasvava jono modulin M alimoduleita, joille pätee $M_i \neq M_{i+1}$. Olkoon N näiden moduleiden yhdiste, $N = \bigcup M_i$. Koska moduleista M_i tiedetään, että $M_1 \subset M_2 \subset \cdots$, on yhdisteen N oltava myös moduli. Nyt kohdasta (N1) seuraa, että N on äärellisesti viritetty. Olkoon $x_1, ..., x_r$ joukon N virittäjät, joista jokainen kuuluu johonkin alimoduliin M_i. Tällöin on olemassa M_j siten. että $x_1, ..., x_r \in M_j$. Nyt

$$\langle x_1, ..., x_r \rangle \subset M_j \subset N = \langle x_1, ..., x_r \rangle.$$

Tästä seuraa, että jono $M_1 \subset M_2 \subset \cdots$, jolle $M_i \neq M_{i+1}$, on äärellinen.

(N2) $\Rightarrow$ (N3): Olkoon S epätyhjä joukko modulin M alimoduleita. Olkoon N_0 joukon S alkio. Jos N_0 ei ole maksimaalinen alkio, niin se sisältyy aidosti johonkin alkioon N_1. Vastaavasti jos N_i ei ole maksimaalinen alkio, niin se sisältyy aidosti johonkin alkioon N_{i+1}. Jos joukossa S ei ole maksimaalista alkiota, niin voimme tällä tavalla muodostaa äärettömän ketjun $N_0 \subset N_1 \subset \cdots$, mikä on kohdan (N2) mukaan mahdotonta. Jokaisen joukon S on siis sisällettävä maksimaalinen alkio.

(N3) $\Rightarrow$ (N1): Olkoon N modulin M alimoduli ja $a_0 \in N$. Jos $N \neq \langle a_0 \rangle$, niin on olemassa $a_1 \in N$ siten, että $a_1 \notin \langle a_0 \rangle$. Jatkamalla tätä, voimme rakentaa seuraavanlaisen jonon modulin N alimoduleita:

$$\langle a_0 \rangle \subset \langle a_0, a_1 \rangle \subset \langle a_0, a_1, a_2 \rangle \subset \cdots .$$

Kohdan (N3) mukaan jokaisessa tällaisessa joukossa $\{\langle a_0 \rangle, \langle a_0, a_1 \rangle, \langle a_0, a_1, a_2 \rangle, ...\}$ on oltava maksimaalinen alkio, joten jono ei voi olla ääretön. Tällöin jonon viimeinen alkio on N ja lisäksi tämä alkio on myös äärellisesti viritetty. $\square$

Lause 5.3 *Olkoon A kommutatiivinen Noetherin rengas. Tällöin polynomirengas $A[X]$ on Noetherin rengas.*

Todistus: Olkoon I polynomirenkaan $A[X]$ ideaali. Olkoon J_i joukko, johon kuuluu 0 ja alkiot $a \in A$, jotka esiintyvät jossain ideaalin I polynomissa

$$a_0 + a_1 X + \cdots + aX^i$$

korkeimman asteen termin kertoimena. Nyt huomataan, että joukko J_i on ideaali: jos $a, b \in J_i$, niin $a \pm b \in J_i$, koska alkioita a ja b vastaavat polynomit kuuluvat ideaaliin I ja näiden polynomien summan/erotuksen korkeimman asteen termin kertoimena on $a \pm b$. Vastaavasti, jos $x \in A$, niin $xa \in J_i$, koska vastaava polynomi kuuluu ideaaliin I. Lisäksi

$$J_0 \subset J_1 \subset J_2 \subset \cdots ,$$

koska jos $a \in J_i$, niin $a \in J_{i+1}$, koska kertomalla joukon J_i alkiota vastaava polynomi muuttujalla X saadaan polynomi, jossa termin X^{i+1} kertoimena on a.

Määritelmän 5.1 mukaan jono ideaaleja J_i päättyy:

$$J_0 \subset J_1 \subset J_2 \subset \cdots \subset J_r = J_{r+1} = \cdots$$

Määritelmän 5.2 tavalla voidaan todistaa, että Noetherin renkaan ideaalit ovat äärellisesti viritettyjä. Olkoon

$$\begin{gathered} a_{01}, ..., a_{0n_0} \text{ ideaalin } J_0 \text{ virittäjät} \\ \vdots \\ a_{r1}, ..., a_{rn_r} \text{ ideaalin } J_r \text{ virittäjät.} \end{gathered}$$

Olkoon f_{ij} astetta i oleva ideaalin I polynomi, jonka korkeimman asteen kertoimena on a_{ij}, missä $i = 0, ..., r$ ja $j = 1, ..., n_i$. Seuraavaksi todistamme, että polynomit f_{ij} ovat ideaalin I virittäjät.

Olkoon $f \in I$ astetta d oleva polynomi. Todistamme induktiolla polynomin asteen d suhteen, että polynomi f kuuluu polynomien f_{ij} virittämään ideaaliin.

Olkoon $d = 0$. Tällöin polynomin aste on nolla, mistä seuraa, että $f_{ij} = a_{ij}$ ja väite pätee, koska tällöin $f \in J_0$ ja tiedetään, että alkiot $a_{01}, ..., a_{0n_0}$ virittävät ideaalin J_0.

Olkoon $d \geq 0$. Jos $d > r$, huomaamme, että polynomien

$$X^{d-r} f_{r1}, ..., X^{d-r} f_{rn_r}$$

korkeimman asteen kertoimet virittävät ideaalin J_d $(= J_r$, koska $d > r)$. Nyt on olemassa alkiot $c_1, ..., c_{n_r} \in A$ siten, että polynomin

$$f - c_1 X^{d-r} f_{r1} - \cdots - c_{n_r} X^{d-r} f_{rn_r}$$

aste on vähemmän kuin d, koska kertoimet c_i voidaan valita siten, että polynomeilla f ja $c_1 X^{d-r} f_{r1} + \cdots + c_{n_r} X^{d-r} f_{rn_r}$ on samat korkeimman asteen kertoimet. Tämä polynomi kuuluu myös ideaaliin I.

Jos $d \leq r$, voimme vastaavasti vähentää polynomista lineaarikombinaation

$$f - c_1 f_{d1} - \cdots - c_{n_d} f_{dn_d}$$

ja saamme polynomin, jonka aste on vähemmän kuin d ja joka kuuluu ideaaliin I. Huomaamme, että polynomi, joka vähennettiin polynomista f kuuluu polynomien f_{ij} virittämään ideaaliin. Toistamalla tätä, voimme löytää polynomien f_{ij} virittämästä ideaalista polynomin g, jolle $f - g = 0$. $\square$

Lause 5.4 *Olkoon M Noetherin A-moduli. Tällöin jokainen modulin M alimoduli ja tekijämoduli ovat Noetherin moduleita.*

Todistus: Alimodulille väite seuraa suoraan määritelmän 5.2 ehdosta (N1). Olkoon N modulin M alimoduli ja $f : M \to M/N$ kanoninen homomorfismi.

Olkoon $N_1 \subset N_2 \subset \cdots$ kasvava jono joukon M/N alimoduleita ja $M_i = f^{-1}(N_i)$. Tällöin lauseesta 4.6 seuraa, että $M_1 \subset M_2 \subset \cdots$ on kasvava jono modulin M alimoduleita. Koska alimodulit M_i ovat modulin M alimoduleita, täytyy jonon olla äärellinen. Tästä seuraa myös, että jonon $N_1 \subset N_2 \subset \cdots$ täytyy olla äärellinen. Nyt määritelmän 5.2 kohdasta (N2) seuraa, että M/N on Noetherin moduli, eli Noetherin modulin tekijämodulit ovat myös Noetherin moduleita. □

Lause 5.5 *Olkoon M moduli ja N alimoduli. Jos N ja M/N ovat Noetherin moduleita, niin M on Noetherin moduli.*

Todistus: Yhdistetään jokaiseen modulin M alimoduliin L seuraavanlainen pari moduleita:

$$L \mapsto (L \cap N, (L+N)/N),$$

missä $L + N = \{l + n \mid l \in L, n \in N\}$. Todistamme väitteen: Jos E ja F ovat modulin M alimoduleita, $E \subset F$ ja niihin yhdistetyt moduliparit ovat samoja, niin $E = F$. Olkoon $x \in F$. Oletuksen nojalla $(E+N)/N = (F+N)/N$, joten on olemassa alkiot $u, v \in N$ ja $y \in E$ siten, että $y+u = x+v$. Nyt

$$x - y = u - v \in F \cap N = E \cap N.$$

Koska $y \in E$, niin myös $x \in E$ ja olemme todistaneet väitteen.

Olkoon $E_1 \subset E_2 \subset \cdots$ kasvava jono modulin M alimoduleita. Tällöin jonon alkioihin yhdistetyt modulien N ja M/N alimoduliketjut ovat äärellisiä, eli on olemassa E_n siten, että $E_i \cap N = E_{i+1} \cap N$ ja $(E_i+N)/N = (E_{i+1}+N)/N$, kun $i \geq n$. Tästä seuraa, että myös $E_i = E_{i+1}$, kun $i \geq n$, siis jonon $E_1 \subset E_2 \subset \cdots$ on oltava äärellinen, mistä määritelmän 5.2 kohdan (N2) nojalla seuraa, että M on Noetherin moduli. □

Lause 5.6 *Olkoon M moduli ja N, N' alimoduleita. Jos $M = N + N'$ ja N, N' ovat Noetherin moduleita, niin M on Noetherin moduli.*

Todistus: Aluksi huomataan, että $N \times N'$ on Noetherin moduli, koska sillä on alimodulina N, jonka tekijämoduli on isomorfinen modulin N' kanssa ja lause 5.5 pätee. Nyt meillä on surjektiivinen homomorfismi

$$N \times N' \to M$$

siten, että pari (x, x'), jossa $x \in N$ ja $x' \in N'$, kuvautuu alkiolle $x+x'$. Koska f on surjektiivinen homomorfismi, tiedetään, että

$$M = Im(f) \cong N \times N'/ker(f),$$

missä $N \times N'$ on Noetherin moduli. Nyt lauseesta 5.4 seuraa, että M on Noetherin moduli. $\square$

Lause 5.7 *Olkoon A Noetherin rengas ja M äärellisesti viritetty A-moduli. Tällöin M on Noetherin moduli.*

Todistus: Aluksi todistetaan, että rengasta A voidaan ajatella Noetherin A-modulina. Todistetaan, että modulin A alimodulit ovat renkaan A ideaaleja, jolloin tiedetään, että modulin A alimodulit täyttävät määritelmän 5.1 mukaan määritelmän 5.2 ehdon (N2).

Olkoon A' modulin A alimoduli. Nyt A' on modulin A aliryhmä, eli $x + y \in A'$ kaikilla $x, y \in A'$. Lisäksi määritelmän 4.2 ehdosta (AM3) seuraa, että $ax \in A'$ kaikilla $a \in A$ ja $x \in A'$, kun toimintana on renkaan A kertolasku. Nyt tiedetään, että modulin A alimodulit ovat renkaan A ideaaleja, mistä seuraa, että A on Noetherin A-moduli.

Olkoon $x_1, ..., x_n$ modulin M virittäjät. Tästä seuraa, että on olemassa homomorfismi

$$f : \underbrace{A \times A \times \cdots \times A}_{n \ kpl} \to M$$

siten, että

$$f(a_1, ..., a_n) = a_1x_1 + \cdots + a_nx_n.$$

Lauseen 5.6 nojalla tulo on Noetherin moduli. Koska $x_1, ..., x_n$ virittävät modulin M, on homomorfismi f surjektio. Tästä seuraa, että

$$M = Im(f) \cong G/ker(f),$$

missä $G = A \times A \times \cdots \times A$ on Noetherin moduli. Nyt lauseesta 5.4 seuraa, että M on Noetherin moduli. $\square$

6 Kuntalaajennokset

Tässä kappaleessa esitellään kuntalaajennoksiin liittyviä määritelmiä ja lauseita, joita tarvitaan nullstellensatzin todistamiseen.

Määritelmä 6.1 *Kunnan K laajennos L on mikä tahansa kunnan K ylikunta, eli kunta, joka sisältää kunnan K alikuntana. Laajennosta merkitään L/K ja kuntaa K kutsutaan laajennoksen lähtökunnaksi.*

Määritelmä 6.2 *Kuntalaajennoksen L/K aste on laajennoksen L dimensio K-vektoriavaruutena. Kuntalaajennos on äärellinen, jos sen aste on äärellinen.*

Määritelmä 6.3 *Olkoon L kunnan K laajennos. Alkiota $a \in L$ kutsutaan algebralliseksi kunnan K suhteen, jos on olemassa nollasta poikkeava polynomi $f \in K[X]$, jolle pätee, että $f(a) = 0$. Jos tällaista polynomia ei ole, sanotaan, että a on transkendenttinen kunnan K suhteen. Jos kaikki laajennoksen L alkiot ovat algebrallisia kunnan K suhteen, sanotaan, että L on algebrallinen kunnan K suhteen, ja laajennosta L/K kutsutaan algebralliseksi laajennokseksi.*

Määritelmä 6.4 *Kunta K on algebrallisesti suljettu, jos jokainen polynomi $f \in K[X]$ jakautuu ensimmäisen asteen tekijöihin renkaassa $K[X]$.*

Lause 6.5 *Olkoon K kunta ja $f \in K[X]$ polynomi, joka ei ole vakio. Tällöin on olemassa kunnan K äärellinen laajennos L, jonka suhteen polynomi f jakautuu ensimmäisen asteen tekijöihin.*

Todistus: Todistetaan lause induktiolla polynomin f asteen suhteen. Kun polynomin f aste on 1, on väite selvä. Oletetaan, että väite pätee polynomeilla, joiden aste on n. Olkoon $f \in K[X]$ astetta $n+1$ oleva polynomi ja p tämän polynomin jaoton tekijä.

Osoitetaan, että $\langle p \rangle$ on maksimaalinen ideaali. Oletetaan, että $\langle p \rangle \subset I$, jollain ideaalilla I. Koska $K[X]$ on pääideaalirengas, pätee $I = \langle g \rangle$, jollain $g \in K[X]$. Nyt $p \in \langle g \rangle$, joten $p = gh$, jollain $h \in K[X]$. Koska p on jaoton, on joko g tai p vakio. Nyt $\langle g \rangle = K[X]$ tai $\langle g \rangle = \langle p \rangle$. Kummassakin tapauksessa $\langle p \rangle$ on maksimaalinen ideaali.

Konstruoidaan kunta $K_1 = K[X]/\langle p \rangle$. Lähtökunta K voidaan samastaa kunnan K_1 alikunnan kanssa, jolloin K_1 on kunnan K laajennos.

Merkitään $\alpha = \overline{X} = X + \langle p \rangle$. Sijoittamalla muuttujan X paikalle $\overline{X}$, polynomi p muuttuu polynomiksi $\overline{p}$. Nyt $p(\alpha) = \overline{p} = 0$, eli α on polynomin p juuri ja siten myös polynomin f juuri. Tästä seuraa, että $f = (X - \alpha) \cdot g$, jollain polynomilla $g \in K_1[X]$. Nyt polynomin g aste on n, joten induktio-oletuksen perusteella löytyy kunnan K_1 äärellinen laajennos L, jonka suhteen polynomi g jakaantuu ensimmäisen asteen tekijöihin. □

Lause 6.6 *Kunta K on algebrallisesti suljettu on yhtäpitävää sen kanssa, että kunnalla K ei ole aitoja algebrallisia laajennoksia.*

Todistus: Todistetaan, että jos kunta K on algebrallisesti suljettu, niin kunnalla K ei ole aitoja algebrallisia laajennoksia. Tehdään vastaoletus, että on olemassa aito algebrallinen laajennos L. Nyt laajennoksessa L on olemassa alkio a siten, että $a \notin K$ ja $f(a) = 0$ jollain $f \in K[X]$. Koska K on algebrallisesti suljettu, on polynomilla f ensimmäisen tekijänä $X - a \in K[X]$. Tästä seuraa, että $a \in K$, mikä on ristiriidassa vastaoletuksen kanssa.

Seuraavaksi todistetaan, että jos kunnalla K ei ole aitoja algebrallisia laajennoksia, niin kunta K on algebrallisesti suljettu. Tehdään vastaoletus, että K ei ole algebrallisesti suljettu. Tällöin on olemassa polynomi $f \in K[X]$, joka ei jakaudu ensimmäisen asteen tekijöihin. Nyt lauseen 6.5 mukaan kunnalla K on olemassa laajennos L, jonka suhteen polynomi f jakautuu ensimmäisen asteen tekijöihin. Lisäksi todistuksesta seuraa, että tämä laajennos on algebrallinen, koska lisätyt alkiot ovat muotoa α, jotka ovat jonkin polynomin $f \in K[X]$ juuria. Nyt kunnalla K on olemassa aito algebrallinen laajennos L, mikä on ristiriidassa oletuksen kanssa. □

7 Radikaalit ja nullstellensatz

Tässä kappaleessa tutkitaan varistojen ja ideaalien välistä suhdetta. Tätä kautta päästään käsiksi radikaaleihin sekä tämän työn aiheeseen, nullstellensatziin.

7.1 Varistot ja ideaalit

Tutkimalla varistoja ja ideaaleja, voimme huomata seuraavanlaisen vastaavuuden:

$$\left\{ \begin{matrix} Alivaristot \\ X \subset \mathbb{A}^n \end{matrix} \right\} \underset{V}{\overset{I}{\rightleftarrows}} \left\{ \begin{matrix} Ideaalit \\ I \subset K[x_1, ..., x_n] \end{matrix} \right\}.$$

Kyseessä ei kuitenkaan ole bijektio. Yhdistetystä kuvauksesta $V \circ I$ saadaan identtinen kuvaus $V(I(X)) = X$, mutta kuvaus $I \circ V$ ei ole injektiivinen eikä surjektiivinen. (Harris, 1992)

Esimerkki 7.1 *Polynomin* $x^2 \in K[x]$ *varisto* $V(x^2)$ *on origo* $0 \in \mathbb{A}^1$*, mutta tämän ideaali on* $\langle x \rangle$ *eikä* $\langle x^2 \rangle$*.*

7.2 Radikaalit ja nullstellensatz

Samassa varistossa arvon nolla saavien polynomien ideaalilla I on seuraavanlainen ominaisuus: Mille tahansa polynomille $f \in K[x_1, ..., x_n]$ pätee, että jos $f^n \in I$ jollain $n \in \mathbb{N}$, niin $f \in I$. Olkoon I ideaali renkaassa R. Joukkoa, joka sisältää kaikki polynomit $f \in R$, joille $f^n \in I$, jollain $n \in \mathbb{N}$, kutsutaan ideaalin I radikaaliksi $r(I)$. Ideaalia I sanotaan radikaaliksi ideaaliksi, jos $I = r(I)$. (Harris, 1992)

Nyt yhdistetyllä kuvauksella $I \circ V$ on seuraavanlainen ominaisuus: $I(V(I)) = r(I)$. Tästä lauseesta käytetään nimeä nullstellensatz. (Harris, 1992) Nullstellensatzista käytetään joskus myös nimeä "Hilbert's theory of zeroes" (Hilbertin nollajoukkolause). Nullstellensatz todistetaan seuraavassa luvussa.

7.3 Hilbertin vastaavuus

Rajoittamalla tämän luvun alussa esitetyn vastaavuuden oikea puoli radikaaleihin ideaaleihin saadaan bijektiivinen vastaavuus:

$$\left\{ \begin{matrix} Alivaristot \\ X \subset \mathbb{A}^n \end{matrix} \right\} \leftrightarrow \left\{ \begin{matrix} Radikaalit\ ideaalit \\ I \subset K[x_1, ..., x_n] \end{matrix} \right\}.$$

Tätä vastaavuutta kutsutaan Hilbertin vastaavuudeksi. Hilbertin vastaavuus on järjestyksen kääntävä: jos $I_1 \subset I_2$, niin $V(I_2) \subset V(I_1)$. Vastaavasti, jos X_1 ja X_2 ovat varistoja, niin $X_1 \subset X_2 \Rightarrow I(X_2) \subset I(X_1)$.(Kahanpää, 2000) Hilbertin vastaavuuden bijektiivisyys seuraa suoraan nullstellensatzista.

8 Todistus

Tässä kappaleessa todistetaan lause 8.7 (nullstellensatz). Ennen tämän todistamista täytyy kuitenkin todistaa lause 8.4 (heikko nullstellensatz). Käyttämällä heikkoa nullstellensatzia, voimme todistaa nullstellensatzin toisen suunnan. Lopuksi vielä todistetaan toinen suunta, joka on huomattavasti yksinkertaisempi. Joissain lähteissä nimitystä heikko nullstellensatz käytetään myös lauseesta 8.3 (Clark), mutta tässä työssä käytetään lähteen 2 (Harris, 1992) mukaista nimeämistä.

8.1 Heikko nullstellensatz

Tässä kappaleessa todistetaan heikko nullstellensatz, jota käytetään myöhemmin nullstellensatzin todistamiseen.

Lemma 8.1 *Olkoon R Noetherin rengas ja $S \supset R$ polynomirenkaan $R[x_1, ..., x_n]$ alirengas. Jos $R[x_1, ..., x_n]$ on äärellisesti viritetty S-modulina, niin S on äärellisesti viritetty R-algebra.*

Todistus: Oletetaan, että alkiot $y_1, ..., y_n \in R[x_1, ..., x_n]$ virittävät polynomirenkaan $R[x_1, ..., x_n]$ S-modulina. Nyt voimme kirjoittaa, että:

$$x_i = \sum a_{i,j} \cdot y_j$$

ja vastaavasti

$$y_i \cdot y_j = \sum b_{i,j,k} \cdot y_k,$$

missä $a_{i,j}, b_{i,j,k} \in S$. Olkoon $S_0 \subset S$ kertoimien $a_{i,j}$ ja $b_{i,j,k}$ virittämä alirengas renkaassa R. Koska S_0 on äärellisesti viritetty renkaassa R, on sen oltava Noetherin rengas (5.7). Näiden relaatioiden nojalla alkiot $y_1, ..., y_n$ virittävät polynomirenkaan $R[x_1, ..., x_n]$ S_0-modulina. Noetherin renkaassa äärellisesti viritetyn modulin alimoduli on äärellisesti viritetty. Tästä seuraa, että S on äärellisesti viritetty S_0-modulina ja siten myös äärellisesti viritetty R-algebra. □

Lemma 8.2 *Olkoon K kunta ja $f, g, h \in K[X]$. Oletetaan, että f on jaoton polynomi, joka jakaa polynomin gh. Tällöin f jakaa polynomin g tai polynomin h.*

Todistus: Lauseen 6.5 todistuksessa on osoitettu, että $\langle f \rangle$ on maksimaalinen ideaali, koska f on jaoton polynomi. Tästä seuraa, että $\langle f \rangle$ on alkuideaali. Se, että f jakaa polynomin gh tarkoittaa, että $gh \in \langle f \rangle$. Tällöin joko $g \in \langle f \rangle$ tai $h \in \langle f \rangle$, eli f jakaa polynomin g tai polynomin h. □

Lause 8.3 *Renkaan $K[x_1, ..., x_n]$ maksimaalinen ideaali m on muotoa $\langle x_1 - a_1, ..., x_n - a_n \rangle$, joillain $a_1, ..., a_n \in K$, missä K on algebrallisesti suljettu.*

Todistus: Aluksi todistetaan väite, että maksimaalinen ideaali m on muotoa $\langle x_1 - a_1, ..., x_n - a_n \rangle$, on yhtäpitävää sen kanssa, että kuntalaajennos $L = K[x_1, ..., x_n]/m = K$.

1) Jos maksimaalinen ideaali m on muotoa $\langle x_1 - a_1, ..., x_n - a_n \rangle$, niin tekijärengas $K[x_1, ..., x_n]/m = K$: Tekijärenkaassa $K[x_1, ..., x_n]/m$ ideaalin m alkiot vastaavat nollia. Tästä seuraa, että $x_i - a_i = 0$, eli $x_i = a_i$. Tämän samastuksen jälkeen jää jäljelle vakiopolynomit, jotka vastaavat kunnan K alkioita. Kunnan K alkiot eivät samastu keskenään, koska ideaali m ei sisällä vakiopolynomeja.

2) Jos tekijärengas $K[x_1, ..., x_n]/m = K$, niin maksimaalinen ideaali m on muotoa $\langle x_1 - a_1, ..., x_n - a_n \rangle$: Koska $K[x_1, ..., x_n]/m = K$, kuuluu x_i jonkin vakion luokkaan. Tästä seuraa, että $[x_i] = [a_i]$, missä $a_i \in K$. Tästä seuraa, että $[x_1 - a_i] = 0$, eli $x_i - a_i \in m$. Nyt $\langle x_1 - a_1, ..., x_n - a_n \rangle \subset m$. Koska tiedetään, että m on maksimaalinen ideaali, ei m sisällä vakiopolynomeja. Tästä seuraa, että $\langle x_1 - a_1, ..., x_n - a_n \rangle = m$.

Koska K on algebrallisesti suljettu ja lauseen 6.6 mukaan algebrallisesti suljetulla kunnalla ei ole aitoja algebrallisia laajennoksia, on tämä yhtäpitävää sen kanssa, että L on algebrallinen kunnan K suhteen.

Uudelleen järjestämällä muuttujat x_i, voimme olettaa, että $x_1, ..., x_k \in L$ ovat algebrallisesti riippumattomia kunnassa K ja $x_{k+1}, ..., x_n$ algebrallisia alikunnassa $K(x_1, ..., x_n) \subset L$. Koska L on näin ollen äärellisesti viritetty $K(x_1, ..., x_k)$-moduli, voimme käyttää lemmaa 8.1 ja päätellä, että puhtaasti transkendenttinen laajennos $K(x_1, ..., x_k)$ on äärellisesti viritetty K-algebra.

Olkoon $z_1, ..., z_l \in L$ kunnan $K(x_1, ..., x_k)$ virittäjät K-algebrana. Nyt voim-

me kirjoittaa, että:

$$z_i = \frac{P_i(x_1, ..., x_k)}{Q_i(x_1, ..., x_k)}$$

joillain polynomeilla P_i ja Q_i. Olkoon $f \in K[x_1, ..., x_k]$ mikä tahansa jaoton polynomi. Oletuksen nojalla voimme kirjoittaa rationaalifunktion $1/f$ muotoa z_i olevien rationaalifunktioiden polynomina. Poistamalla nimittäjät, voimme päätellä lemman 8.2 avulla, että funktion f täytyy jakaa vähintään yksi polynomeista Q_i, koska f jakaa muotoa Q_i olevien polynomien tulon:

$$\frac{Q_1^{p_1}...Q_l^{p_l}}{f} = \text{Polynomi},$$

joillain $p_1, ..., p_n$. Tästä seuraa, että polynomirenkaassa $K[x_1, ..., x_k]$ on äärellinen määrä jaottomia polynomeja, koska polynomeja Q_i on äärellinen määrä. Lisäksi tiedetään, että jos $k \geqslant 1$, niin polynomirenkaassa $K[x_1, ..., x_k]$ on ääretön määrä jaottomia polynomeja, koska kunta K on ääretön ja voidaan tutkia muotoa $\{x - a\}_{a \in K}$ olevia polynomeja. Kunta K on ääretön, koska äärellinen kunta ei voi olla algebrallisesti suljettu. Tämä seuraa siitä, että äärellisessä kunnassa polynomilla $(x - a_1)(x - a_2)...(x - a_n) + 1$, missä $a_1, ...a_n$ ovat kaikki kunnan alkiot, ei olisi nollakohtia eikä näin ollen ensimmäisen asteen tekijöitä.

Tästä voidaan päätellä, että $k = 0$. Tästä seuraa, että jos L on algebrallinen kunnan K suhteen, niin $L = K$. Tämä taas todistettiin yhtäpitäväksi sen kanssa, että maksimaalinen ideaali m on muotoa $\langle x_1 - a_1, ..., x_n - a_n \rangle$. □

Lause 8.4 (Heikko nullstellensatz) *Ideaali $I \subset K[x_1, ..., x_n]$, jonka polynomeilla ei ole yhteisiä nollakohtia on koko joukko $K[x_1, ..., x_n]$.*

Todistus: Lauseen 8.3 mukaan jokaiselle maksimaaliselle ideaalille m on piste $(a_1, ..., a_n) \in K^n$, joka on jokaisen funktion $f \in m$ nollakohta. Tästä seuraa, että jos ideaalilla ei ole yhteisiä nollakohtia, niin ideaali ei voi sisältyä mihinkään maksimaaliseen ideaaliin, eli ideaalin on oltava koko joukko $K[x_1, ..., x_n]$. □

8.2 Nullstellensatz

Tässä kappalessa todistetaan nullstellensatz molempiin suuntiin. Ensimmäinen suunta saadaan todistettua edellisessä kappaleessa todistetun heikon

nullstellensatzin avulla.

Tämän jälkeen haluamme päätellä lauseen 8.7 (nullstellensatz) toisen suunnan, jonka jälkeen nullstellensatz on todistettu.

Lause 8.5 *Kaikille ideaaleille $I \subset K[x_1, ..., x_n]$ pätee*

$$I(V(I)) \subset r(I).$$

Todistus: Olkoon $I \subset K[x_1, ..., x_n]$ mikä tahansa ideaali ja $f \in K[x_1, ..., x_n]$ mikä tahansa polynomi, jolle pätee, että $f \in I(V(I))$. Nyt haluamme todistaa, että $f^m \in I$ jollain $m \in \mathbb{Z}_+$.

Tämän todistamiseen käytetään Rabinowitschin temppua. Tutkitaan komplementtia $U_f = \{(x_1, ..., x_n) | f(x_1, ..., x_n) \neq 0\} \subset K^n$. Koska komplementissa polynomi $f \neq 0$, saadaan tätä joukkoa vastaava varisto lisäämällä yksi koordinaatti seuraavalla tavalla:

$$\Sigma = \{(x_1, ..., x_{n+1}) | x_{n+1} \cdot f(x_1, ..., x_n) = 1\} \subset K^{n+1}.$$

Nyt huomataan, että ideaalin I ja polynomin $x_{n+1} \cdot f(x_1, ..., x_n) - 1$ virittämän ideaalin $J \subset K[x_1, ..., x_{n+1}]$ polynomeilla ei ole yhteisiä nollakohtia, koska $x_{n+1} \cdot f(x_1, ..., x_n) - 1$ on määritelty siten, että sillä ei ole yhteisiä nollakohtia ideaalin I polynomien kanssa ($f \in I(V(I)) \supset I$). Käyttämällä lausetta 8.4 (heikko nullstellensatz), voimme todeta, että tämän ideaalin täytyy olla koko joukko $K[x_1, ..., x_{n+1}]$.

Koska I ja $x_{n+1} \cdot f(x_1, ..., x_n) - 1$ ovat ideaalin $J = K[x_1, ..., x_{n+1}]$ virittäjät, on olemassa kertoimet $c_1, ..., c_{n+1} \in K[x_1, ..., x_{n+1}]$ siten, että

$$1 = c_1 f_1 + c_2 f_2 + \cdots + c_n f_n + c_{n+1}(x_{n+1} \cdot f(x_1, ..., x_n) - 1)$$

missä $f_1, ..., f_n \in I$.

Sijoittamalla $x_{n+1} = 1/f$ ja kertomalla nimittäjät pois saadaan tämä muotoon

$$f^m = b_1 f_1 + \cdots + b_n f_n,$$

missä $b_i = c_i f^m$. Nyt $b_i \in K[x_1, ..., x_n]$, koska nimittäjät (x_{n+1}) on kerrottu pois. Tästä seuraa, että $f^m \in I$. $\square$

Lopuksi todistamme vielä nullstellensatzin toisen suunnan, jotta saamme todistettua koko nullstellensatzin.

Lause 8.6 *Kaikille ideaaleille* $I \subset K[x_1, ..., x_n]$ *pätee*

$$r(I) \subset I(V(I)).$$

Todistus: Olkoon polynomi f joukon $r(I)$ alkio. Radikaalin määritelmän perusteella tiedetään, että on olemassa positiivinen kokonaisluku a, jolle pätee, että $f^a \in I$. Koska $a \neq 0$, tiedetään myös, että $f = 0$ jos, ja vain jos $f^a = 0$. Tästä seuraa, että $f(x) = 0$, kun $x \in V(I)$. Tästä seuraa, että $f \in I(V(I))$. Nyt on todistettu, että jos $f \in r(I)$, niin $f \in I(V(I))$. Siis

$$r(I) \subset I(V(I)). \square$$

Lause 8.7 (Nullstellensatz) *Kaikille ideaaleille* $I \subset K[x_1, ..., x_n]$ *pätee*

$$I(V(I)) = r(I).$$

Todistus: Seuraa suoraan lauseista 8.5 ja 8.6. $\square$

9 Seurauslauseita

Nullstellensatzista käytetään usein myös seuraavanlaista muotoa:

Lause 9.1 *Jokainen polynomirenkaan $K[x_1, ..., x_n]$ alkuideaali on muotoa $\langle x_1 - a_1, ..., x_n - a_n \rangle$ olevien ideaalien leikkaus.*

Todistus: Todistetaan aluksi, että jokainen alkuideaali A on radikaali, eli $A = r(A)$. Suunta $A \subset I(V(A)) = r(A)$ on selvä.

Olkoon $r \in r(A)$, eli $r^n \in A$, jollain $n \in \mathbb{N}$. Todistetaan induktiolla eksponentin n suhteen, että kaikilla $n \in \mathbb{N}$ ja $r \in K[x_1, ..., x_n]$ pätee, että $r^n \in A \Rightarrow r \in A$. Kun $n = 1$, on väite selvä ($r \in A \Rightarrow r \in A$).

Oletetaan, että väite pätee eksponentilla n ja todistetaan, että $r^{n+1} \in A \Rightarrow r \in A$. Olkoon $r^{n+1} \in A$. Tästä seuraa, että $r \cdot r^n \in A$. Nyt $r \in A$ tai $r^n \in A$, koska A on alkuideaali. Induktio-oletuksen perusteella väitteestä $r^n \in A$ seuraa, että $r \in A$. Nyt on todistettu, että $A = r(A)$.

Olkoon $f \notin A$. Nyt ideaalin A kaikilla polynomeilla on nollakohta b, joka ei ole polynomin f nollakohta, koska muuten $f \in I(V(A)) = r(A) = A$. Olkoon $m = I(\{b\})$. Tämä on maksimaalinen ideaali, koska $\langle m, g \rangle$ on koko joukko $K[x_1, ..., x_n]$ kaikilla polynomeilla $g \notin m$, koska polynomilla g ei voi olla yhteisiä nollakohtia jokaisen ideaalin m polynomin kanssa. Tästä seuraa, että m on sellainen maksimaalinen ideaali, että $A \subset m$ ja $f \notin m$. Nyt A on kaikkia polynomeja $f \notin A$ vastaavien ideaalien m leikkaus ja lauseen 8.3 mukaan jokainen maksimaalinen ideaali m on muotoa $\langle x_1 - a_1, ..., x_n - a_n \rangle$. □

Lause 9.2 *Jokainen radikaali ideaali $I \subset K[x_1, ..., x_n]$ voidaan yksikäsitteisesti muodostaa äärellisen monen alkuideaalin A_i leikkauksena, missä $A_i \nsubseteq A_j$, jos $i \neq j$*

Todistus: Tehdään vastaoletus: on olemassa joukko radikaaleja ideaaleja $I \subset K[x_1, ..., x_n]$, jotka eivät ole äärellinen leikkaus alkuideaaleista. Tässä todistuksessa käytämme tietoa, että Noetherin renkaassa jokainen ideaalijoukko $\{J_i\}$ sisältää maksimaalisia alkioita (seuraa suoraan määritelmästä 5.1). Koska nullstellensatzin (lause 8.7) mukaan kaikki radikaalit ovat myös ideaaleja, voimme tätä käyttää tietoa joukkoon radikaaleja ideaaleja I. Olkoon I_0 maksimaalinen tällainen ideaali. Tästä valinnasta seuraa, että I_0 ei

voi olla alkuideaali.

Olkoon $a, b \in K[x_1, ..., x_n]$ sellaisia polynomeja, jotka eivät kuulu ideaaliin I_0, mutta $ab \in I_0$. Olkoon

$$I_1 = r(I_0, a) \quad ja \quad I_2 = r(I_0, b)$$

ideaalin I ja alkioiden a ja b virittämien ideaalien radikaaleja. Koska radikaalit ideaalit I_1 ja I_2 sisältävät radikaalin ideaalin I_0, on niiden vastaoletuksen perusteella oltava äärellisen monen alkuideaalin leikkaus, koska muuten I_0 ei olisi maksimaalinen radikaali ideaali, joka ei ole äärellisen monen alkuideaalin leikkaus.

Seuraavaksi haluamme todistaa, että

$$I_0 = I_1 \cap I_2.$$

Olkoon $f \in I_1 \cap I_2$. Määritelmästä 2.5 seuraa, että on olemassa $f^m \in (I_0, a)$ ja $f^n \in (I_0, b)$, jollain $m, n \in \mathbb{N}$. Nyt voimme kirjoittaa, että

$$f^m = g_1 + h_1 \cdot a \quad ja \quad f^n = g_2 + h_2 \cdot b,$$

missä $g_1, g_2 \in I_0$. Mutta nyt

$$f^{m+n} = g_1 g_2 + g_1 h_2 b + g_2 h_1 a + h_1 h_2 \cdot ab \in I_0.$$

Koska I_0 on radikaali, seuraa tästä, että $f \in I_0$, siis $I_0 = I_1 \cap I_2$. Koska tiedetään, että I_1 ja I_2 ovat molemmat äärellisen monen alkuideaalin leikkauksia, on myös ideaalin I_0 oltava äärellisen monen alkuideaalin leikkaus, mikä on ristiriidassa vastaoletuksen kanssa. □

10 Lähteet

1. Lauri Kahanpää, Karen E. Smith ja Pekka Kekäläinen: Johdattelua algebralliseen geometriaan, Yliopistokustannus, 2000

2. Joe Harris: Algebraic geometry: a first course, Springer, 1992.

3. Serge Lang: Algebra, Addison-Wesley, 1992

4. Jokke Häsä: Algebra II, Matematiikan ja tilastotieteen laitos, kevät 2010, Helsingin yliopisto
http://wiki.helsinki.fi/download/attachments/70230320/AlgII.pdf?version=1&modificationDate=1327072149612

5. Jokke Häsä ja Johanna Rämö, Johdatus abstraktiin algebraan, Gaudeamus, 2012.

6. Pete Clark: The nullstellensatz; Closed points and k-points, University of Georgia
http://www.math.uga.edu/~pete/8320notes3.pdf